INCIDENT RESPONSE PLAN

JUSTICE LEAGUE INC.

Course	INFO6081
Date	03 June 2023
Group 14	
Gihan Shamike Liyanage	1142109
Deepik Ravichander	1144695
Saiganesh Jeyapandi	1154547
Shanjeevan Mahesapalan	1126696

Disclosure of Assumptions

For the purpose of this report some assumptions were made with the intention to provide realistic business as usual elaboration.

Assumptions as follows:

1. The name of the organization this incident response plan was made is for Justice League Inc.
2. Employee names, details, organization structure and vendors.
3. Details pertaining to scenario 1, scenario 2 and scenario 3 that are mentioned in the appendix.

Table of Contents

1 Document Version Control

Version	Change Description	Created By	Approved By	Approved Date
1.0	1. Introduction 2. Terminology and Definitions 3. Roles and Responsibilities 4. Incident Response Process a. Detection b. Containment	Shanjeevan Mahesapalan	CSO	June 01 2023
1.1	1. Appendix A: Resolution Action Plan Log (Scenario 1: Unauthorized Access) 2. Review and sign off Appendix A, B, C 3. Incident Response Process a. Analysis b. Post-incident Activity	Gihan Shamike Liyanage	CSO	June 02 2023
1.2	1. Incident Response Process a. Eradication b. Recovery 2. Appendix B: Resolution Action Plan Log (Scenario 2: System Intrusion)	Saiganesh Jeyapandi	CSO	June 02 2023
1.3	1. Incident Response Process a. Post-incident Activity 2. Appendix C: Resolution Action Plan Log (Scenario 3: Physical Security Breach)	Deepika Ravichander	CSO	June 03 2023

2 Introduction

2.1 Purpose

The purpose of this incident response plan is to provide a guided approach to manage IT security incidents, with the utmost intention to prevent or limit the damage. This document was developed referring to various industry best practices which are cited in respective sections of this document.

2.2 Authority

The custodians of this incident response plan is the cyber security incident response team (CSIRT) of the organization. Accountability to the adherence to the plan as well as ensuring the availability of a reliable secure IT environment lies with the Chief Security Officer (CSO) of the organization.

2.3 Review

A review of this plan will be conducted in below mentioned instances.

- Annual review of this plan by the CSIRT team.
- After encountering a high severity incident, following a thorough impact analysis.

3 Terminology and Definitions

This section will set definitions and terminologies that are deemed necessary for this plan.

3.1 Cyber incident

A cyber incident is an occurrence of an action that threatens the confidentiality, integrity, or availability of any digital asset of the organization.

#	Incident Type	Description
1	Unauthorized Access	• An external party, attempting or gaining access to the corporate network / Digital assets / Systems. • An insider attempting to access or accessing corporate network / Digital assets / Systems they don't have access to.
2	System Intrusion	Unauthorized access to corporate network or systems exploiting the vulnerabilities, with the intention to tamper the data, gain control or perform malicious activities.
3	Physical Security Breach	• An external party gaining unauthorized access to physical office locations or entering office premises where they are not permitted to. • An insider gaining unauthorized access to physical office locations or entering office premises where they are not permitted to. • An unauthorized personal, gaining access to a digital device of the organization. • Digital device of an organization being stolen, by an external party or insider.
4	Ransomware Attacks	A malware that encrypts the data in corporate digital asset / individual pc by making in inaccessible to anyone until the ransom is paid to the attacker.
5	Malware Infection	Introduction of a malware infection into corporate digital assets in the form of viruses, worms, trojans or spyware leading to data loss or system disruption.
6	Denial of Service (DOS) or Distributed Denial of Service (DDOS)	An attack to the corporate network or applications by flooding data traffic or requests which leads to making the assets inaccessible to legitimate users.
7	Phishing and Social Engineering	Deceiving users to gain unauthorized access or disclose sensitive information.
8	Advanced Persistent Threats	Complex and prolonged attacks by threat agents, targeting corporate digital assets with the intention for stealing valuable corporate insights, data or intellectual property.

3.2 Threat Agents

Cyber incidents originate through various threat agents. Below are some potential threat agents applicable to some of the identified incident types.

#	Threat Agent	Description
1	Hackers	Individuals or group attempts to gain unauthorized access to organization network / digital assets.
2	Malicious / Unauthorized Insiders	Individuals within the organization who access organization network / digital assets by abusing their empowerments with the intention to disrupt the business operations and cause damage.
3	Criminals	Any external individual or group that is involved in various forms of crime, attempts to gain unauthorized physical access with the intention to steal digital assets of the organization.
4	Natural Disasters	Natural events such as earthquake, fire, flood or storms that can cause physical damage to the infrastructure or disrupt services.

3.3 Incident Severity

Based on the anticipated impact each incident must be tagged a severity level which is expected to be done by the member of IT operations team member at the IT support desk, however, it is subjected to change at any level by IR manager. Incident severity will dictate the SLAs for first response, resolution time, as well as the resource allocation.

Severity Level	Description
High	Attributes to one of the below mentioned: - Severe damage, corruption, loss of confidential business data or customer specific data. - Extended loss of system/s or network resource/s across the entire business sector. - Damage to the corporate public image. Potential damage or liability to the organization.
Moderate	Attributes to one of the below mentioned: - Damage, corruption, loss of replaceable information without compromise or misuse of sensitive customer information. Extended loss of system/s or network resource/s in one single business unit.
Low	Attributes to one of the below mentioned: - Causes only a minor disruption or inconvenience to the business. Unintentional damage or loss of recoverable information.

3.4 Incident SLA

3.4.1 First Response

Severity Level	Response Time
High	< 10 minutes
Moderate	< 60 minutes
Low	< 8 Hours

3.4.2 Resolution

Severity Level	Resolution Time
High	< 4 Hours
Moderate	< 6 Business Hours
Low	< 36 Business Hours

4 Roles and Responsibilities

This section provides necessary information of the roles and responsibilities of all involved stakeholders during an incident response. This section also lists the external stakeholders whom the team can reach out to, for further support.

4.1 CSIRT Team

A central CSIRT has been established for this purpose, where end to end incident process will be executed by the team.

Name	Contact Details	Role	Responsibility
Bruce Wayne	411 411 4111 Bruce.Wayne@jl.ca	IR Manager	• Oversee response process. • Coordinate among CSIRT team as well as external members. • Determine incident priorities.
Billy Batson	411 411 4112 Billy.Batson@jl.ca	Organization Security Manager	• Investigation of incidents. • Law enforcement liaison.
Victor Stone	411 411 4113 Victor.Stone@jl.ca	Forensic Analyst	• Custodian for digital evidence. • Leading investigation on collected digital evidence.
Clark Kent	411 411 4114 Clark.Kent@jl.ca	Communication Manager	• Internal and stakeholder communications. • Media and community liaison.
Barry Allen	411 411 4115 Barry.Allen@jl.ca	Legal Advisor	• Legal and compliance advisory.
Diana Prince	411 411 4116 Diana.Prince@jl.ca	IT Operations Lead	• Respond to incident through ticket system JIRA. • Escalate to respective CSIRT team member.

Arthur Curry	411 411 4117 Arthur.Curry@jl.ca	IT System Admin Lead	• Implement necessary response measures. • Update lessons learnt repository as well as the necessary config changes that were performed in configuration documentation.
John Stewart	411 411 4118 John.Stewart@jl.ca	CSO	• Decisions pertaining to business continuity related matters.

4.2 External Stakeholders

Below listed are the external stakeholders who can be approached for further support and guidance.

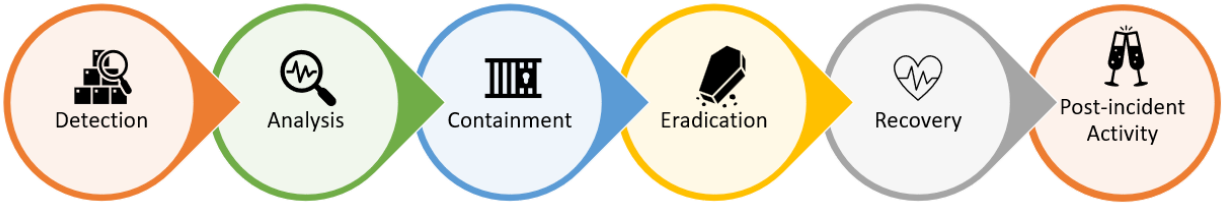
Name	Contact Details	Role	Responsibility
Canadian Centre for Cyber Security	833 232 3788 contact@cyber.gc.ca	Government Level Escalation Point for Further Legal Advisory	• Legal and expert advisory assistance.
Amanda Waller	422 422 4222 Amanda.Waller@ssquad.ca	SPOC Firewall Vendor (The S Squad LLC)	• Activate extended support agreement by deploying senior level resources for expert advice.
Lex Luther	423 423 4333 Lex.Luther@lexcorp.ca	SPOC of ISP provider (Lex Corp)	• Activate manage service agreement by assigning expert advisors.

4.3 Steering Committee

Name	Contact Details	Role	Responsibility
Jerry Siegel	433 433 4223 Jerry.Siegel@jl.ca	CIO	• Advisory in maintaining overall IT strategic alignment.
Bob Kane	433 433 4224 Bob.Kane@jl.ca	CFO	• Advisory on managing financial risk exposure.
John Stewart	411 411 4118 John.Stewart@jl.ca	CSO	• Advisory on overall cyber security strategic alignment.
William Moulton	411 411 4119 William.Moulton@jl.ca	CRO	• Advisory on corporate risk management.

5 Incident Response Process

The incident response process consists of six process areas that are shown below. This section will elaborate on each process area.



All six process areas are derived from the best practices mentioned in the computer security incident handling guide published by National Institute of Standards and Technology.

5.1 Detection

This process phase is the critical phase where downstream processes are triggered for further action by respective process owners. Trigger for an incident will fall into one of the below mentioned two categories (Cichonski, Millar, Grance, & Scarfone, 2012).

1. Precursors – an indication for a possible incident. Below are some possible scenarios.
    a. Server log entries of a vulnerability scanner.
    b. Receipt of a threat from an individual or group of an attack.
    c. News or announcement of a global malware or ransomware attack.
2. Indicators – an indication that an incident has occurred or is presently occurring. Below are some examples.
    a. System administrator witnesses a filename that contains an unusual name or character.
    b. Alert from the antivirus of a malware infection.
    c. Application log / alert of multiple failed login attempts from an unknown remote system.
    d. System administrator notices of large number of bounced emails with contents that raises suspicious.
    e. User notices that his / her application screen being redirected to a fake login page.

Triggers originate from various types of sources such as alerts, logs, publicly available information, and people. Section 5.1.1 explores some of the possible sources that are incorporated for IR detection.

5.1.1 Sources of Precursors and Indicators

There are various triggering points for both precursors and indicators. Below listed are some common sources indicated by NIST (Cichonski, Millar, Grance, & Scarfone, 2012).

Type	Source
Alerts	• Antivirus applications. • File integrity checking software applications. • Third party monitoring services. • Security information and event management applications.
Logs	• Operating system logs. • Active directory logs. • Services and application logs.

	• Network device logs
Public Information	• Common vulnerabilities and exposure published on https://www.cve.org/. • Microsoft security bulletins. • Latest advisories and alerts on the website of Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en.
People	• Internal stakeholders – Employees. • External stakeholders – Vendors, External Consultants. • People from other organizations. • Well known industry experts.

5.1.2 Reporting the Incident

The vital next step of the detection will be reporting through the ticketing system, so that it can be taken over by the next process step analysis. Reporting is expected to be done by the corporate incident reporting system JIRA that is made available to all employees. From raising the ticket in JIRA every single action taken pertaining to the incident should be recorded under the respective ticket as a comment, not only that but also approvals, sign offs or clearances should also be obtained through the JIRA ticket management system. This will help trace back any history in the future, as well as will help with the lesson learnt documentation as part of the post incident activity phase.

JIRA ticket is configured to capture vital mandatory information at each level of journey of the ticket.

5.2 Analysis

Once the incident is reported by the originator, the IT support desk that is handled by the IT operations team will assign the severity level, do the first response, and perform an analysis considering the indicators of a potential cyber incident. Below mentioned process steps will be executed to confirm the presence of a cyber incident.

#	Action
1	Refer to the below mentioned technical documentations that is applicable to the circumstance and identify any deviations from the baseline. • Network diagrams • IP lists • Port lists • Documentations pertaining to system architecture diagrams and configurations
2	Review log entries and application alerts for unusual entries or suspicious behavior.
3	Refer to operating system wise Standard Operating Procedures and identify and deviations.
4	Consult system / network administrator team to validate any deviations from the baseline found in the documentations.
5	Conduct research referring to publicly available information mentioned in section 5.1.1, in order to make sure, and review the same to firm the occurrence of an incident.
6	Formulate the list of suspected IPs or user accounts and monitor their ongoing activity.
It's important to note that there shouldn't be any communication made to the suspected IP address or URL from the corporate network.	

7	Through the above steps, if deemed that the incident is indeed a cyber incident, IT incident handler can update the incident
8	From this point onwards CSIRT team will take the responsibility by moving onto the next process step Containment.

5.3 Containment

The containment plan is as important as any process phase, the intention of this process is to limit the damage before the impact hits the risk appetite of the organization (Johansen, Digital Forensics and Incident Response : A Practical Guide to Deploying Digital Forensic Techniques in Response to Cyber Security Incidents, 2017). This is achieved by isolating the affected system from the corporate network. In this phase critical decision making is required and two key people are empowered to make decisions related to the containment strategy that is to be activated.

Empowerment for decision making lies with the following CSIRT members.

Level	CSIRT Member
Primary	IR Manager
Secondary – when the primary is unavailable	IT System Admin Lead

Industry best practice is to maintain incident type specific containment strategies. Below mentioned are some major incidents and the containment strategy that should be activated. For incidents that are not mentioned here, IR manager should be consulted on further action.

Incident Type	Containment Strategy
Cyber Security Incidents	**Phishing Attack** • Remove phishing emails from the mail server. • Block the originating email and the domain address of the mail from reaching user mailboxes. Retain at server level for further investigation. **Ransomware Attack** • Disconnect infected system from the corporate network. • Configure firewall rules to block suspected ransomware sources. **Data Breach** • Based on the identified vulnerability during analysis phase, identify the asset that contains the vulnerability and isolate it from the corporate network and take it offline from any external connectivity. • Redirect attacker/s to the sandbox environment so that further evidence can be gathered for investigations. Before executing this, its vital to ensure that sandbox environment is completely isolated from corporate network, so that further attack cannot be executed using this environment as a medium.

	One important constraint to consider when isolating the affected host asset is, necessary measures has to be taken to the asset in the next process phases to prevent further damages to the host asset.
Physical Security Incidents	**Theft / Loss of Physical Assets** • Make all attempts to perform successful remote wipe. • Report to law enforcement for investigation and recovery. **Unauthorized Access** • Restrict access to the high-risk corporate premise by deploying more security or reviewing access controls to all entry points to the respective premise.
Operational Incidents	**Data Loss** • Take the respective system offline to prevent financial loss or data contamination, that may lead to integrity issues of the data.

Once the incident is successfully contained and no further disruptions are ensured, the incident can be moved to the next phase eradication.

5.4 Eradication

Eradication is a critical phase that involves removing the threat from the affected digital asset. This involves identifying and addressing the vulnerability and removing the threat (Microsoft Service Assurance | Microsoft Learn, 2023). Depending on the incident type one or combination of the below streamlined strategies must be activated.

Incident Type	Eradication strategies
Cyber Security Incidents	**Isolate Affected Systems:** • Determine which systems were impacted. • Isolate the affected systems. Prioritize the isolation of critical system essential to daily operation. **Removal of Malware:** • Delete the temporary files using Disk Cleanup tool. This will speed up the process during malware-scan. • Run a scan using an anti-malware scanner and identify the threat. • Remove the malicious file or software. • Check the application settings, whether it's modified by the malware. **Patch and Update Systems:** • Check and identify all the systems and applications that the organization uses. • Observe various sources of information to check the patches or updates are legit. • Once the patch or update is released, it should be tested and evaluated in a controlled environment before deploying it into the actual system. • Verify the patches and updates whether it's correctly installed and if it's working as expected after the deployment. • Keep a record of patches and update installed. This can help with troubleshooting future issues.

	Hardening of System: • Configure the system in a way that only a limited number of the users and programs can access the permission to perform the duties. • Audit the systems regularly. Review the logs to detect and respond to recent security incidents. • Reset passwords and authentication tokens for all identified victim accounts and enable muti-factor authentication. **Reimage affected system:** • Quarantine or take offline potentially affected hosts. • Reimage compromised system to remove any threats.
Physical Incidents	**Physical Access Controls:** • Use Preventive controls such as fences, locks, security guards, security cameras and similar measures. They are the first line of defense in securing a facility or resource. • Use Detective Controls that detect and alert when an unauthorized access or intrusion occurs. These include motion detectors, alarm systems and CCTV systems that record activity for later review. • Corrective controls are used to restore systems to normal state after incident. These include backup systems or disaster recovery plans to respond to breaches. **Secure Disposal of Hardware:** • In some cases, disposal of physical hardware is necessary as some sensitive data cannot be deleted. • This should be carried out by a professional service that can provide a certificate of destruction. • Keep a record of secure disposal for each piece of hardware. This includes the process of data wiping and destruction process. **Secure Configurations:** • Physical devices need to be securely configured. • This includes disabling unnecessary services, encrypting data at rest or physically securing devices to prevent theft or tampering.

5.5 Recovery

Recovery is restoring systems to BAU working status and ensuring that the systems are functioning as per the standard operating procedures. Recovery may involve one or a combination of the following activities.

#	Action
1	Restoring systems with a clean backup.
2	Rebuilding the entire application eco system from the scratch.
3	Installing patches.
4	Changing passwords or affected / suspected user accounts.
5	Tightening network security configurations.
6	Confirm the impacted systems are functioning normally.

7	Implement short term / long term monitoring strategy.

Implementation of short term / long term monitoring mechanism is quite important, as the probability of the same asset being attacked again is on the higher end.

In the event where recovery is expected to take more than a month, a timeline specific phased out approach should be implemented with the below mentioned approach. Approach was derived from the computer security incident handling guide published by National Institute of Standards and Technology.

Phase #	Action	Timeline
Phase 1	Increase overall asset security, by initiating high value configurational changes, in order to prevent similar incidents.	3 Business Days
Phase 2	Upon completion of phase 1, initiate long term configurations / changes / continuous improvements.	Agreed timeline with the steering committee.

5.6 Post-incident Activity

This is considered the most important process phase of an incident response plan, in the perspective of prevention of an incident in similar nature. This phase has three elements, that are recording lessons learned, collected incident data and evidence retention (Cichonski, Millar, Grance, & Scarfone, 2012).

5.6.1 Lessons Learned

Each incident helps the CSIRT team to evolve by gaining new knowledge on new threats and new technologies. This immense amount of tacit knowledge is vital to build a sustainable secure corporate infrastructure by reviewing the details of each incident, the actions taken to mitigate them. This must be initiated by a meeting within two business days following the resolution of the incident.

Below are some indicative discussion points that could be used as an agenda for this discussion. Outcomes of these points should be documented in the action plan log as shown in Appendix A, B and C.

#	Discussion Points
1	What were the specific details of the incident, including the sequence of events and the exact times they occurred?
2	How effectively did the staff and management handle the incident?
3	What information was required earlier in the incident response process?
4	Were there any actions or measures taken that may have impeded the recovery process?
5	What would the staff, management and incident response team do differently if a similar incident were to happen again?
6	What corrective actions can be implemented to prevent similar incidents from occurring in the future?
7	What additional tools or resources are necessary for better detection, analysis, and mitigation of future incidents?

5.6.2 Evidence Retention

There are two purposes that should be focused on evidence retention. Firstly, for any sort of legal prosecutions or internal employee inquiries. Until the prosecution or the internal employee inquiry is concluded evidence should be retained safely and securely as primary evidence.

Secondly, as per the data retention policy of the organization all digital data should be retained for 1068 days (3 years). In compliance with the policy necessary measures should be taken to obtain data backups and stored as per the backup policy. Evidence includes physical evidences such as hard drives and removable media that are used to hold disk images, log files, database backups, reports generated by IDS and antivirus.

Appendix A, B and C elaborates detailed action plan for the three types of cyber incidents, that template action plan log will also be used to update for every incident ticket as a supporting document to keep a trace of all actions performed.

6 Appendix A: Resolution Action Plan Log (Scenario 1: Unauthorized Access)

Detection

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
The intrusion detection analyst promptly initiates communication with the incident response team upon identifying the incoming connection originating from the IP address listed in the watchlist.		
Identified individual to create a JIRA ticket with detailed description.		
The incident response team acknowledges the alert and initiates the incident response process		

Analysis

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Confirm the authenticity of the intrusion detection alert.		
Confirm the watchlist IP address and the connection to the organization's VPN server.		
Collect and preserve relevant logs, including intrusion detection, firewall, and VPN server logs.		
Determine the authenticated user ID for the session and the name of the associated user.		
Conduct a thorough analysis of the logs to understand the extent of the intrusion, potential system vulnerabilities, and the actions taken by the intruder.		
Access if any sensitive data or systems have been compromised, severity of incident and impact of the intrusion.		
Document the findings and create a timeline of the incident to support containment and eradication steps.		

Containment

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Isolate the affected VPN server from the network to prevent further unauthorized access.		
Disable or block the user accounts associated with the malicious activity		
Review and update firewall rules to block traffic from the watchlist IP address		
Implement additional access controls and monitoring the network traffic for any suspicious or ongoing activities if necessary		

Eradication

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Perform a comprehensive scan of the affected systems to identify any malware or malicious artifacts left behind		
Remove any malware, suspicious files, or unauthorized access points from affected systems		
Patch or update any identified vulnerabilities to prevent similar incidents in the future.		
Review and update security configurations, including the VPN server, firewalls, and intrusion detection systems.		

Recovery

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Restore the impacted VPN server to a previously verified, secure state and validate its integrity to ensure its functionality and security.		
Validate the integrity and security of other critical systems and applications.		
Perform a comprehensive review of the network infrastructure to identify and address any remaining security vulnerabilities.		

Post-incident Activity

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Record the occurrence, including a timeline of what occurred, what was performed, and what was discovered.		
Inform applicable stakeholders, such as management, legal, and any regulatory authorities if required.		
Conduct a post-incident review to identify areas of improvement in incident response procedures and preventive measures.		
Update the incident response plan based on the insights and lessons learned from the recent intrusion		

7 Appendix B: Resolution Action Plan Log (Scenario 2: System Intrusion)

Detection

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Discover the unfamiliar directory names and files contacts the incident response team immediately.		
User to create a JIRA ticket with detailed description.		
The incident response team initiates a secure communication channel to discuss and coordinate the incident response.		

Analysis

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Gathers information from the database administrator regarding the discovered directories and files		
Assess the severity and potential impact of the unauthorized access		
Evaluate the impending data or system vulnerabilities that may have been exploited.		

Containment

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Promptly segregate the compromised database server from the network to avert any additional unauthorized access.		
Deactivate any compromised accounts or user access linked to the attacker		
Enforce supplementary access controls (IP restrictions or two-factor authentication) to fortify the defense against subsequent unauthorized access attempts.		
Evaluate and revise firewall rules to obstruct any suspicious network traffic linked to the attacker		

Eradication

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Remove any malicious files, scripts, or unauthorized modifications from the compromised asset.		
Apply patches or updates to address any identified vulnerabilities.		
Change all passwords and access credentials associated with the compromised server		
Conduct a comprehensive review of security configurations, including user permissions, network settings, and access controls		

Recovery

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Restore the compromised database server to a previously verified and trusted state that is known to be secure.		
Perform a thorough examination of the server and database configurations to identify and remediate any remaining security vulnerabilities or gaps.		
Validate the integrity and security of other critical systems and applications that may have been impacted.		

Post-incident Activity

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Document the incident, including a timeline of events, actions taken, and findings.		
Specify recommendations for advancing security controls and practices to prevent similar events in the future.		
Ensure compliance with all applicable legal and regulatory reporting obligations related to the incident.		
Notify applicable stakeholders, management, legal, and any regulatory authorities if required.		
Conduct a post-incident review to identify areas of improvement in incident response procedures and preventive measures.		
Update the incident response plan based on lessons learned		

8 Appendix C: Resolution Action Plan Log (Scenario 3: Physical Security Breach)

Detection

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Identifying a movement of mouse or any evidence of physical intrusion and apprise the incident response team		
User to create a JIRA ticket with detailed description.		
The incident response team observe the criticality of the incident and initiates the incident response process		

Analysis

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Analyzing **payroll** software **event** logs based on the timestamp of event occurrence		
Check pc event logs to identify any unauthorized changes		
Examining of payroll database server logs to understand a possible change in the pay roll data.		
Examine footages of CCTVs and Biometrics access-control devices data to identify the intruder.		
Preserve the potential evidence left behind by the intruder for further analysis.		

Containment

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Isolate the payroll administrator’s devices from the corporate network.		
Disable or temporarily suspend the user account of the payroll administrator as a precautionary measure.		

Eradication

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Sanitizing the pay roll and other possible business critical software.		
Changing the credentials of the payroll administrator's workstation and the affected hosts on the network		
Initiate a system scan across all relevant devices and network endpoints to detect and identify any potentially malicious software or unauthorized applications that may have been installed		

Recovery

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
If necessary, restoring the systems to its previous state by using the backups.		
Reloading the pay role applications with controlled access on the administrator's workstation		

Post-incident Activity

Action	Action performed by: [Member / System]	Action performed at: [Date & Time]
Validating the security policies		
Root cause analysis of the incident		
Update the group policies to enforce preventive measures and mitigate the risk of unattended PCs being utilized for unauthorized activities.		
Update the incident response plan based on the incident.		
Conduct training sessions or reminders for employees, including the payroll administrator, on security best practices		

9 References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). Computer Security Incident Handling Guide. *Special Publication 800-61 Revision 2*. Gaithersburg, United States of America: National Institute of Standards and Technology. Retrieved from NIST Technical Series Publications: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Johansen, G. (2017). In G. Johansen, *Digital Forensics and Incident Response : A Practical Guide to Deploying Digital Forensic Techniques in Response to Cyber Security Incidents* (pp. 20-22). Packt Publishing, Limited.

Johansen, G. (2017). Digital Forensics and Incident Response. In G. Johansen, *APractical Guide to Deploying Digital Forensic Techniques in Response to Cyber Security Incidents* (pp. 19-25). Birmingham: Packt Publishing, Limited.

Microsoft Service Assurance | Microsoft Learn. (2023, June 03). Retrieved from Microsoft security incident management: Containment, eradication, and recovery - Microsoft Service Assurance: https://learn.microsoft.com/en-us/compliance/assurance/assurance-sim-containment-eradication-recovery